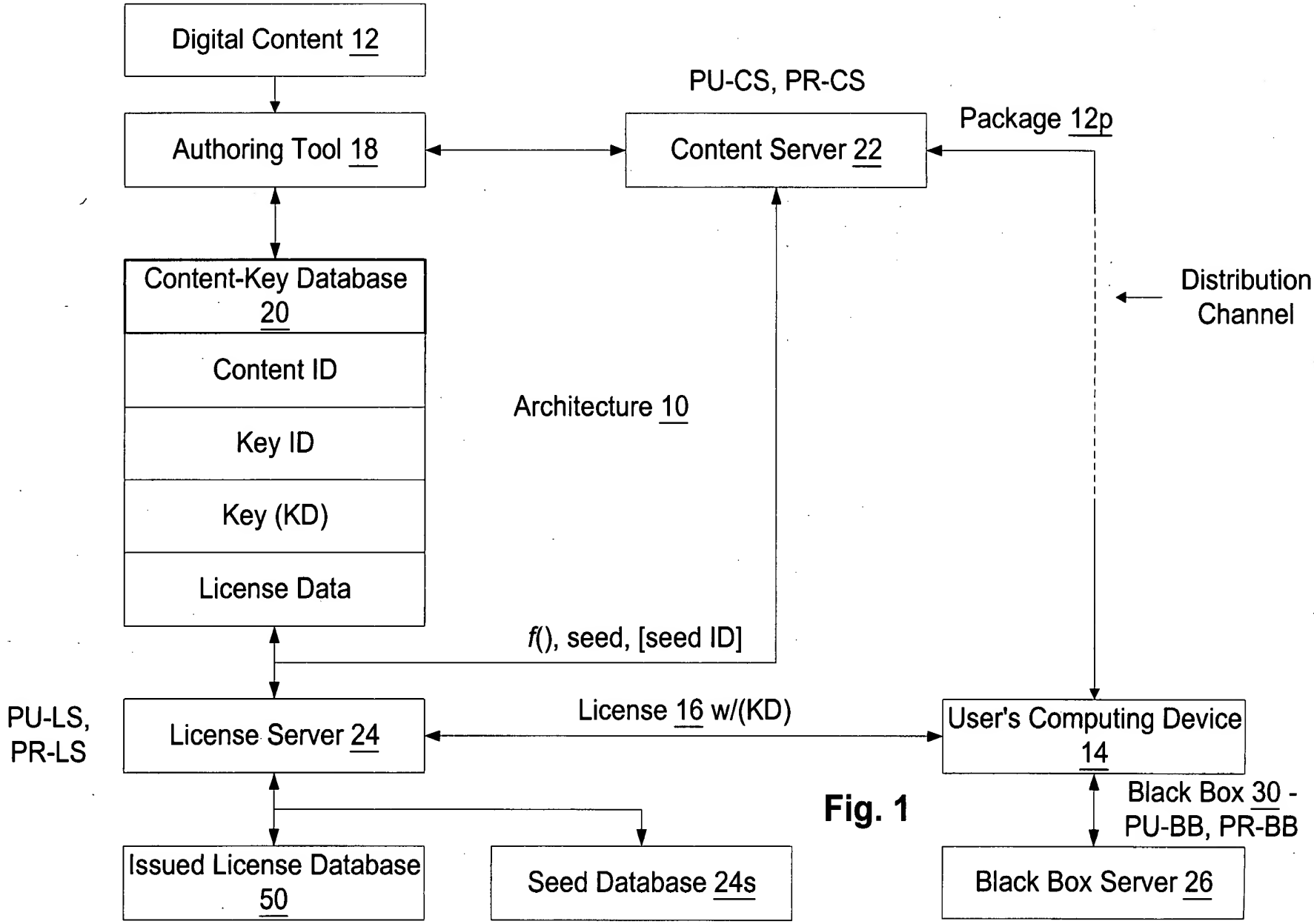
Digital Content 12
Authoring Tool 18
Content-Key Database 20
Content ID
Key ID
Key (KD)
License Data
PU-CS, PR-CS
Content Server 22
Package 12p
Distribution Channel
Architecture 10
f(), seed, [seed ID]
PU-LS, PR-LS
License Server 24
License 16 w/(KD)
User's Computing Device 14
Black Box 30 - PU-BB, PR-BB
Issued License Database 50
Seed Database 24s
Black Box Server 26

Fig. 1

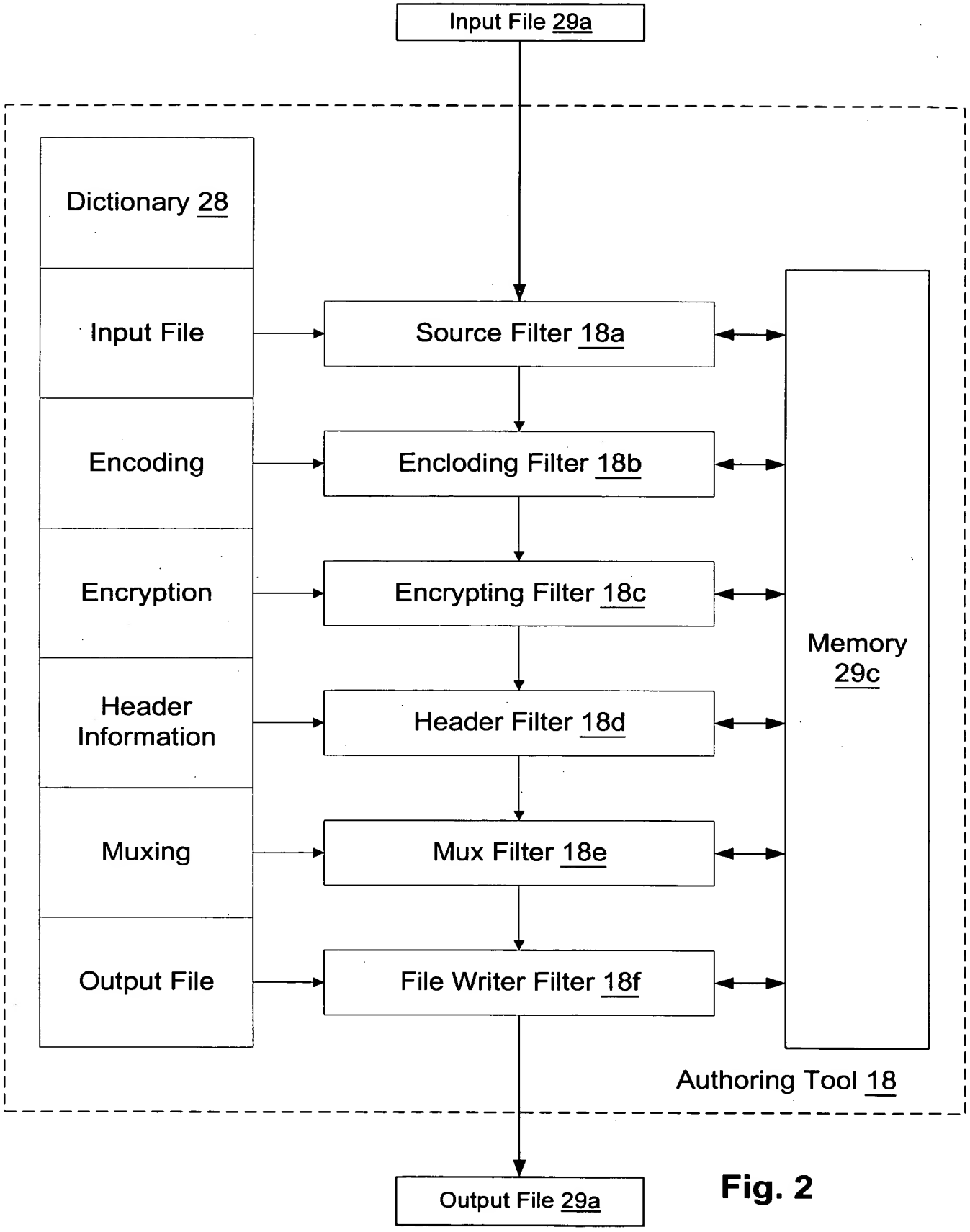
Input File 29a
Dictionary 28
Input File
Encoding
Encryption
Header Information
Muxing
Output File
Source Filter 18a
Encloding Filter 18b
Encrypting Filter 18c
Header Filter 18d
Mux Filter 18e
File Writer Filter 18f
Memory 29c
Authoring Tool 18
Output File 29a

Fig. 2

Scanned Document

Digital Content Package 12p
KD (Digital Content 12)
Content ID
Key ID
[Seed ID]
License Acquisition Info
KD (PU-CS) S (PR-CS)

Fig. 3

License 16
Content ID
DRL 48 or KD (DRL 48)
PU-BB (KD)
S (PR-LS)
CERT (PU-LS) S (PR-CS)
Security Requirement 68
Trusted Security Value Cert. Auth. 74

Fig. 8

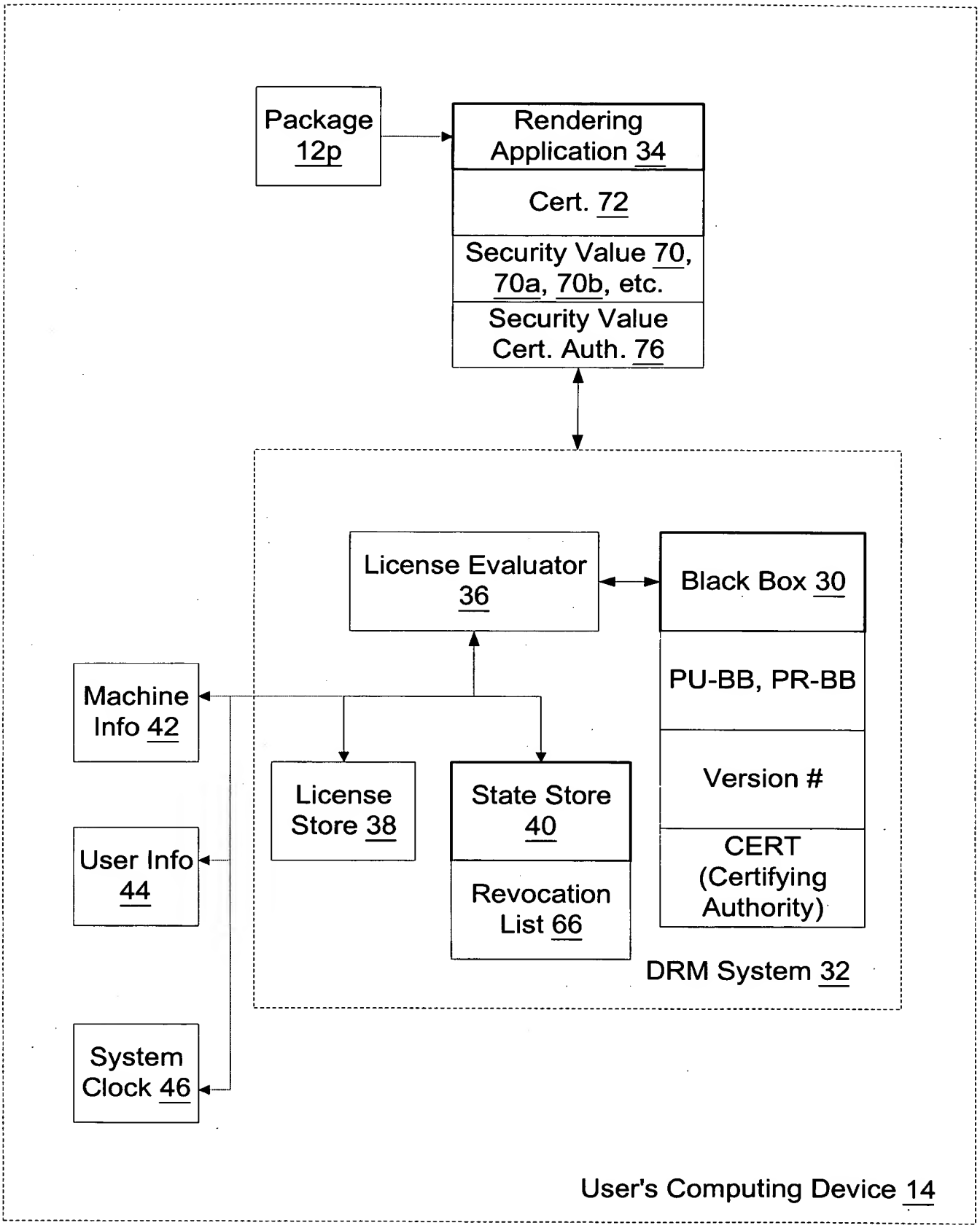
Package 12p
Rendering Application 34
Cert. 72
Security Value 70, 70a, 70b, etc.
Security Value Cert. Auth. 76
License Evaluator 36
Black Box 30
PU-BB, PR-BB
Version #
CERT (Certifying Authority)
Machine Info 42
License Store 38
State Store 40
Revocation List 66
User Info 44
System Clock 46
DRM System 32
User's Computing Device 14

Fig. 4

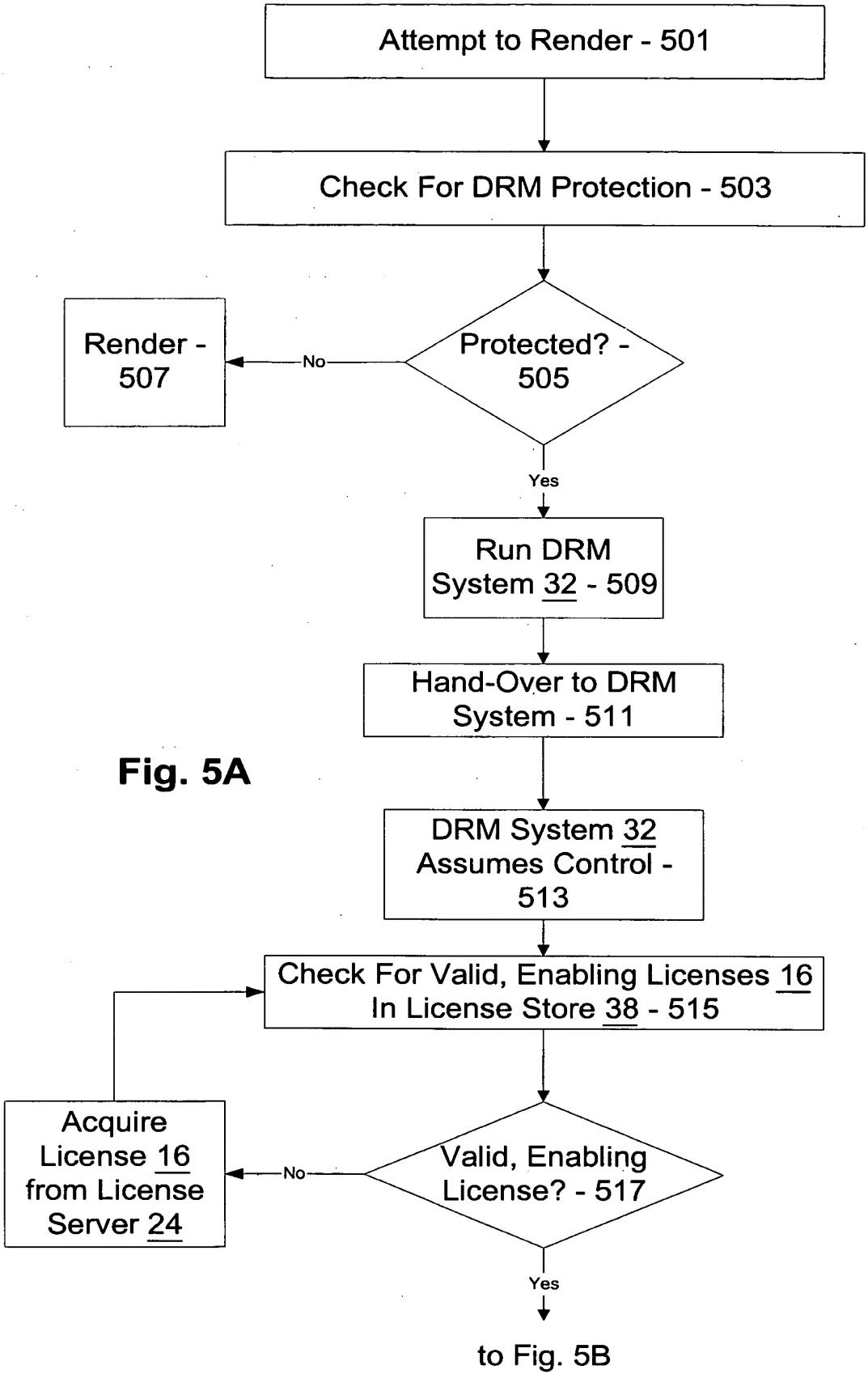
Attempt to Render - 501
Check For DRM Protection - 503
Protected? - 505
No
Render - 507
Yes
Run DRM System 32 - 509
Hand-Over to DRM System - 511
DRM System 32 Assumes Control - 513
Check For Valid, Enabling Licenses 16 In License Store 38 - 515
Valid, Enabling License? - 517
No
Acquire License 16 from License Server 24
Yes
to Fig. 5B

Fig. 5A

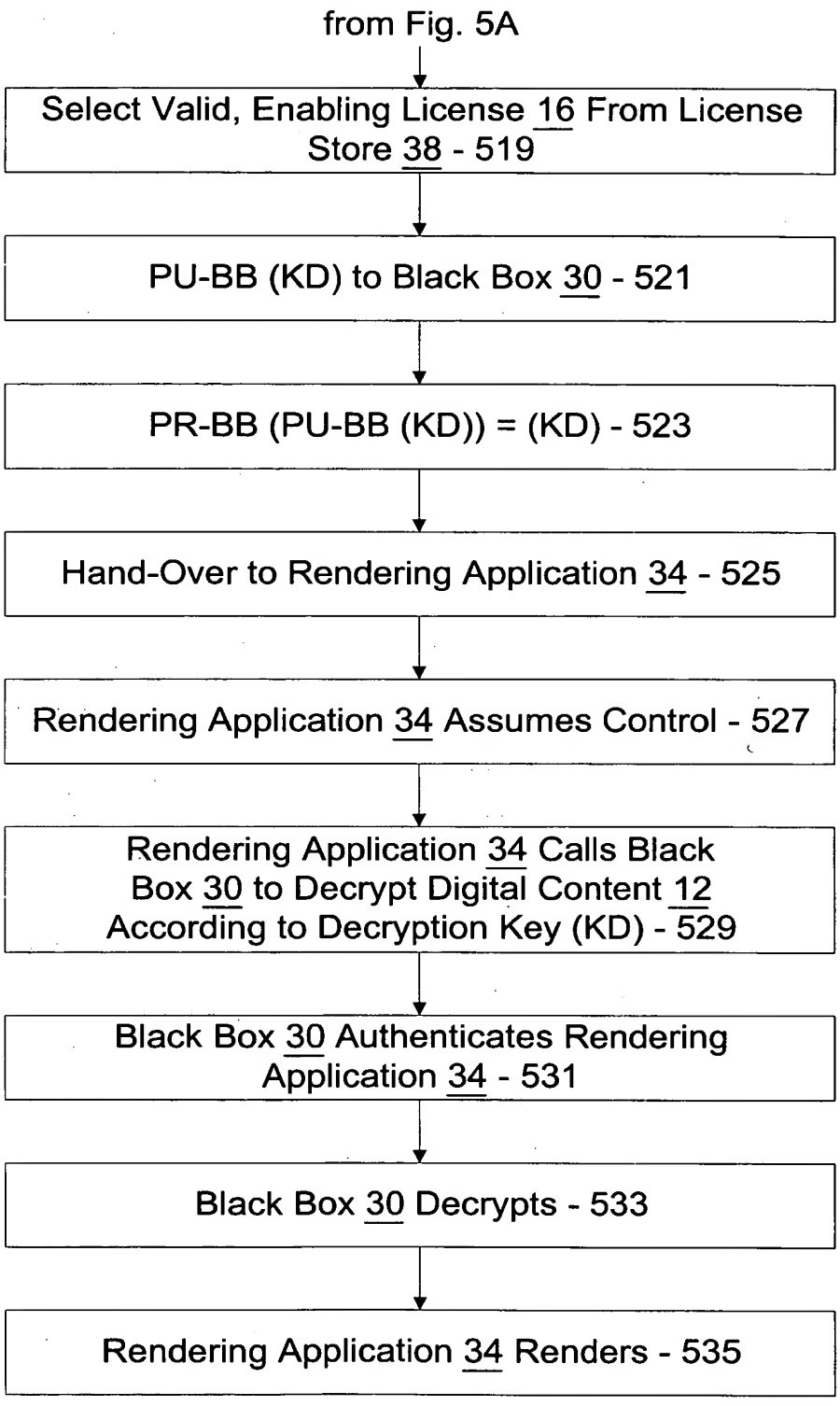
from Fig. 5A
Select Valid, Enabling License 16 From License Store 38 - 519
PU-BB (KD) to Black Box 30 - 521
PR-BB (PU-BB (KD)) = (KD) - 523
Hand-Over to Rendering Application 34 - 525
Rendering Application 34 Assumes Control - 527
Rendering Application 34 Calls Black Box 30 to Decrypt Digital Content 12 According to Decryption Key (KD) - 529
Black Box 30 Authenticates Rendering Application 34 - 531
Black Box 30 Decrypts - 533
Rendering Application 34 Renders - 535

Fig. 5B

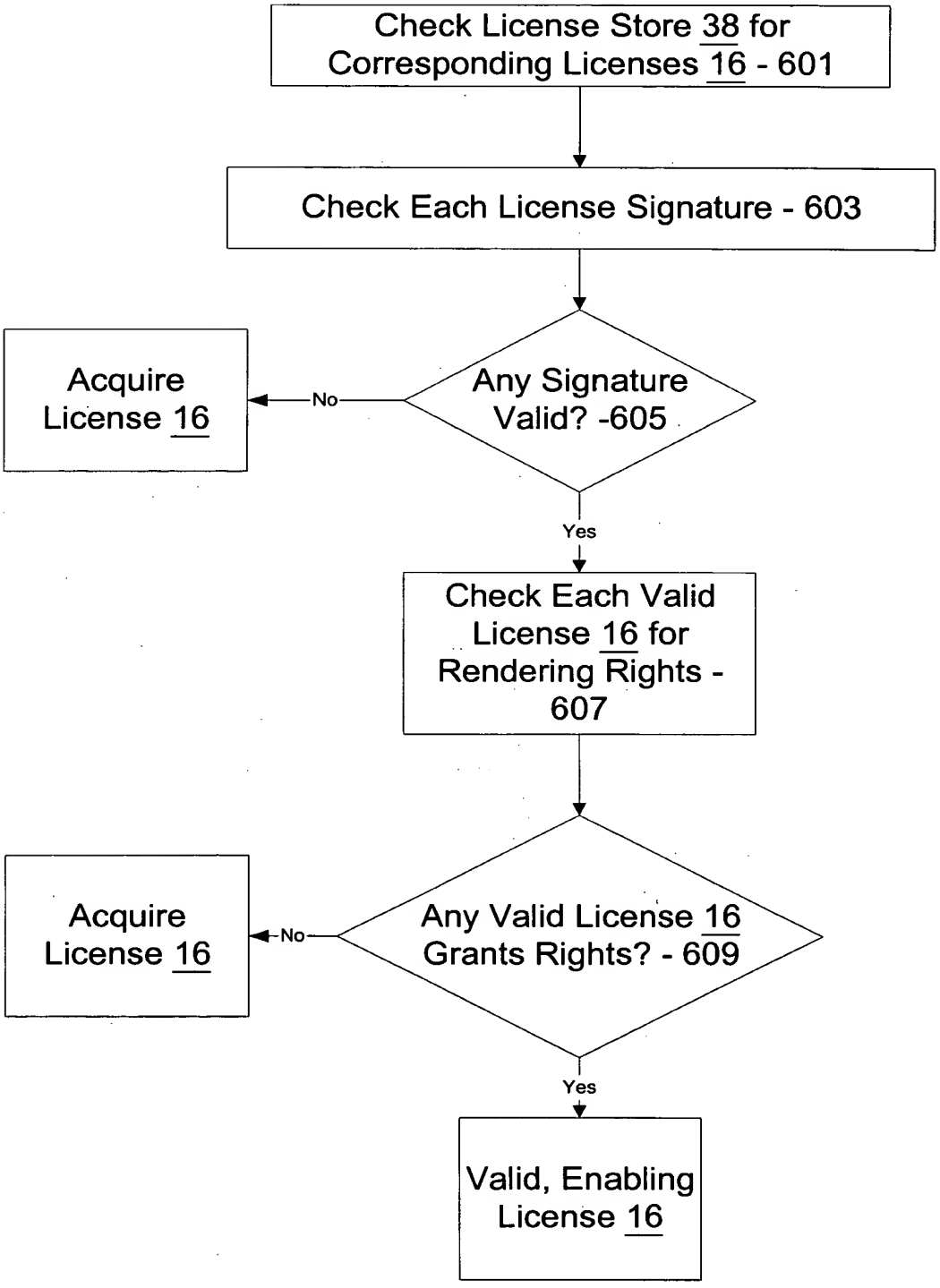
Check License Store 38 for Corresponding Licenses 16 - 601
Check Each License Signature - 603
Any Signature Valid? -605
No
Acquire License 16
Yes
Check Each Valid License 16 for Rendering Rights - 607
Any Valid License 16 Grants Rights? - 609
No
Acquire License 16
Yes
Valid, Enabling License 16

Fig. 6

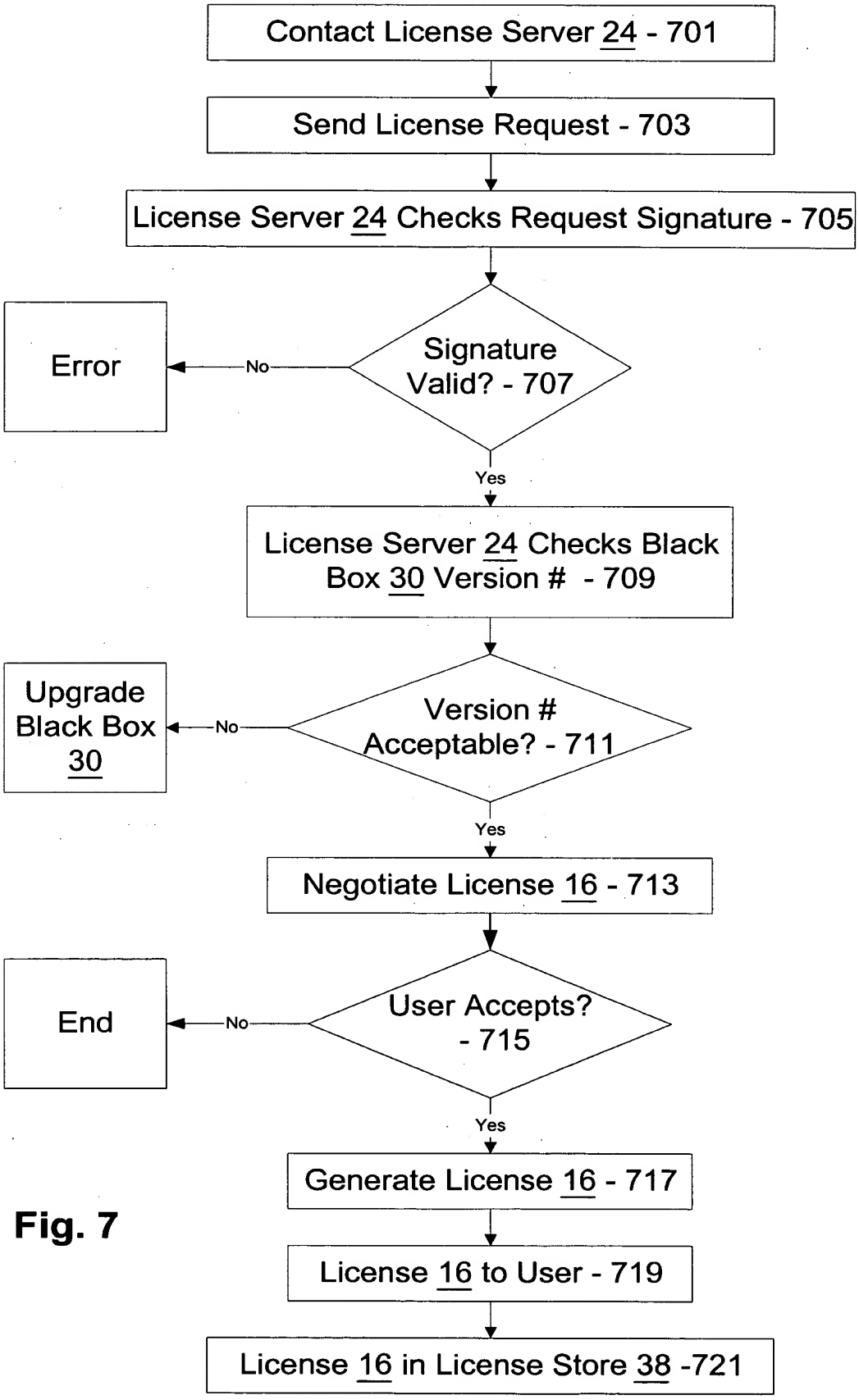
Contact License Server 24 - 701
Send License Request - 703
License Server 24 Checks Request Signature - 705
Signature Valid? - 707
No
Error
Yes
License Server 24 Checks Black Box 30 Version # - 709
Version # Acceptable? - 711
No
Upgrade Black Box 30
Yes
Negotiate License 16 - 713
User Accepts? - 715
No
End
Yes
Generate License 16 - 717
License 16 to User - 719
License 16 in License Store 38 -721

Fig. 7

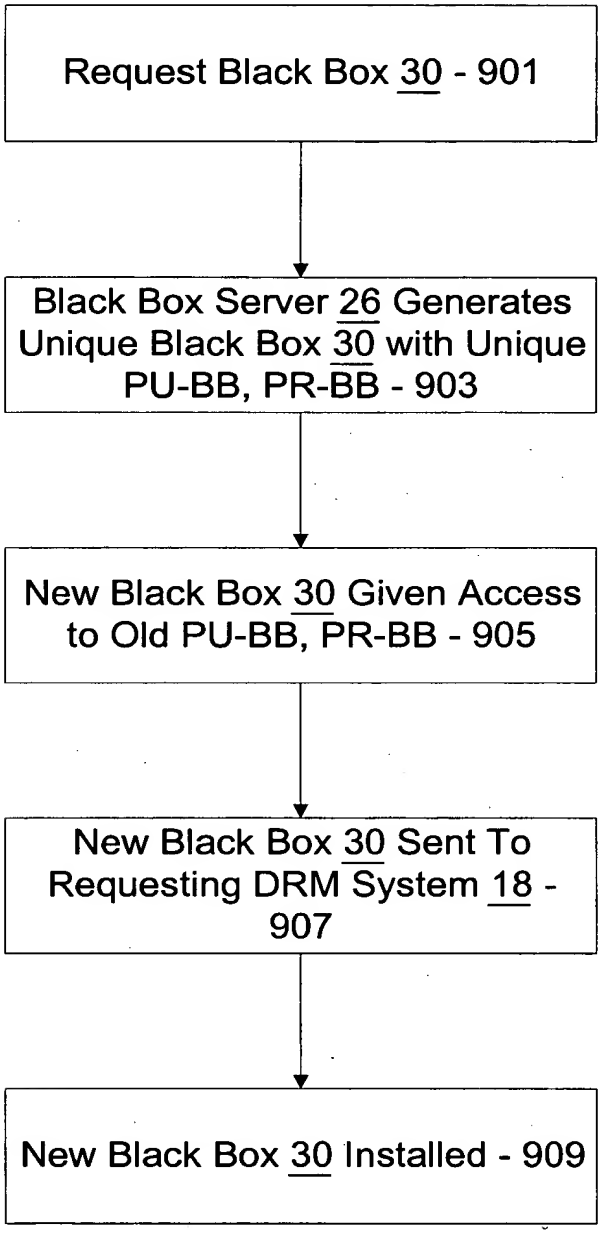
Request Black Box 30 - 901
Black Box Server 26 Generates Unique Black Box 30 with Unique PU-BB, PR-BB - 903
New Black Box 30 Given Access to Old PU-BB, PR-BB - 905
New Black Box 30 Sent To Requesting DRM System 18 - 907
New Black Box 30 Installed - 909

Fig. 9

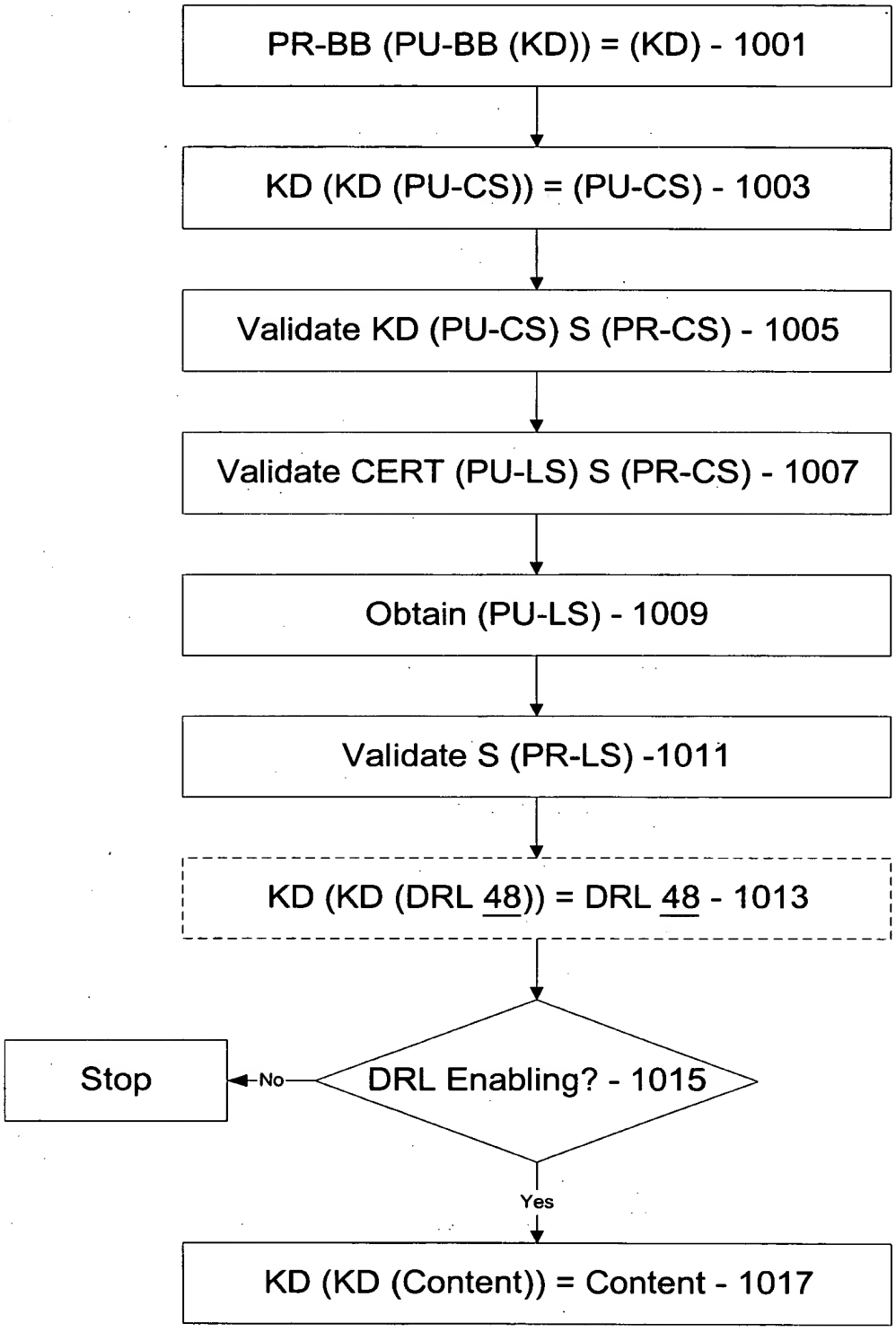
PR-BB (PU-BB (KD)) = (KD) - 1001
KD (KD (PU-CS)) = (PU-CS) - 1003
Validate KD (PU-CS) S (PR-CS) - 1005
Validate CERT (PU-LS) S (PR-CS) - 1007
Obtain (PU-LS) - 1009
Validate S (PR-LS) -1011
KD (KD (DRL 48)) = DRL 48 - 1013
DRL Enabling? - 1015
No
Stop
Yes
KD (KD (Content)) = Content - 1017

Fig. 10

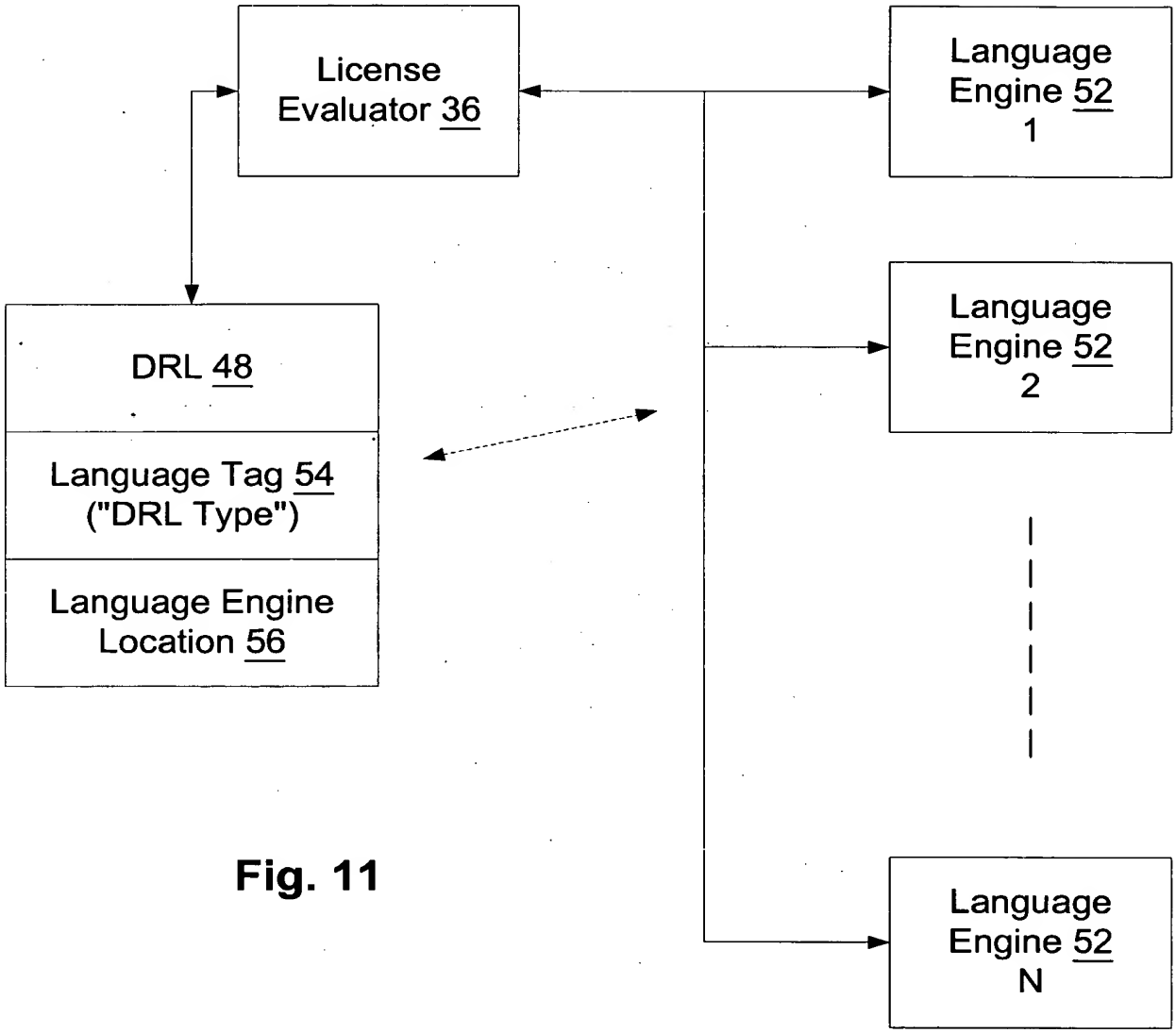
License Evaluator 36
Language Engine 52 1
Language Engine 52 2
Language Engine 52 N
DRL 48
Language Tag 54 ("DRL Type")
Language Engine Location 56

Fig. 11

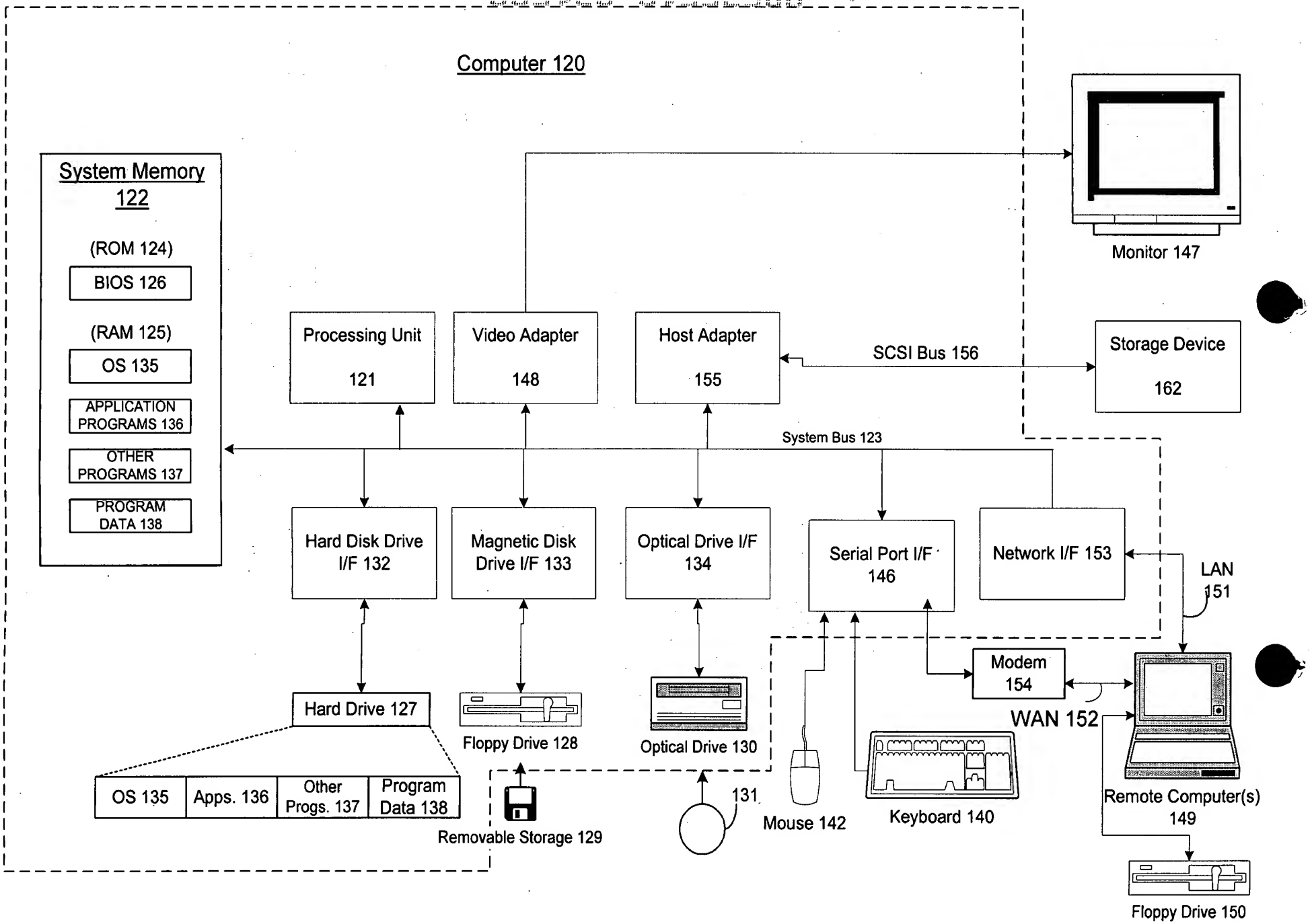
Computer 120
System Memory 122
(ROM 124)
BIOS 126
(RAM 125)
OS 135
APPLICATION PROGRAMS 136
OTHER PROGRAMS 137
PROGRAM DATA 138
Processing Unit 121
Video Adapter 148
Host Adapter 155
SCSI Bus 156
Storage Device 162
Monitor 147
System Bus 123
Hard Disk Drive I/F 132
Magnetic Disk Drive I/F 133
Optical Drive I/F 134
Serial Port I/F 146
Network I/F 153
LAN 151
Modem 154
WAN 152
Hard Drive 127
Floppy Drive 128
Optical Drive 130
OS 135
Apps. 136
Other Progs. 137
Program Data 138
Removable Storage 129
131
Mouse 142
Keyboard 140
Remote Computer(s) 149
Floppy Drive 150

Fig. 12

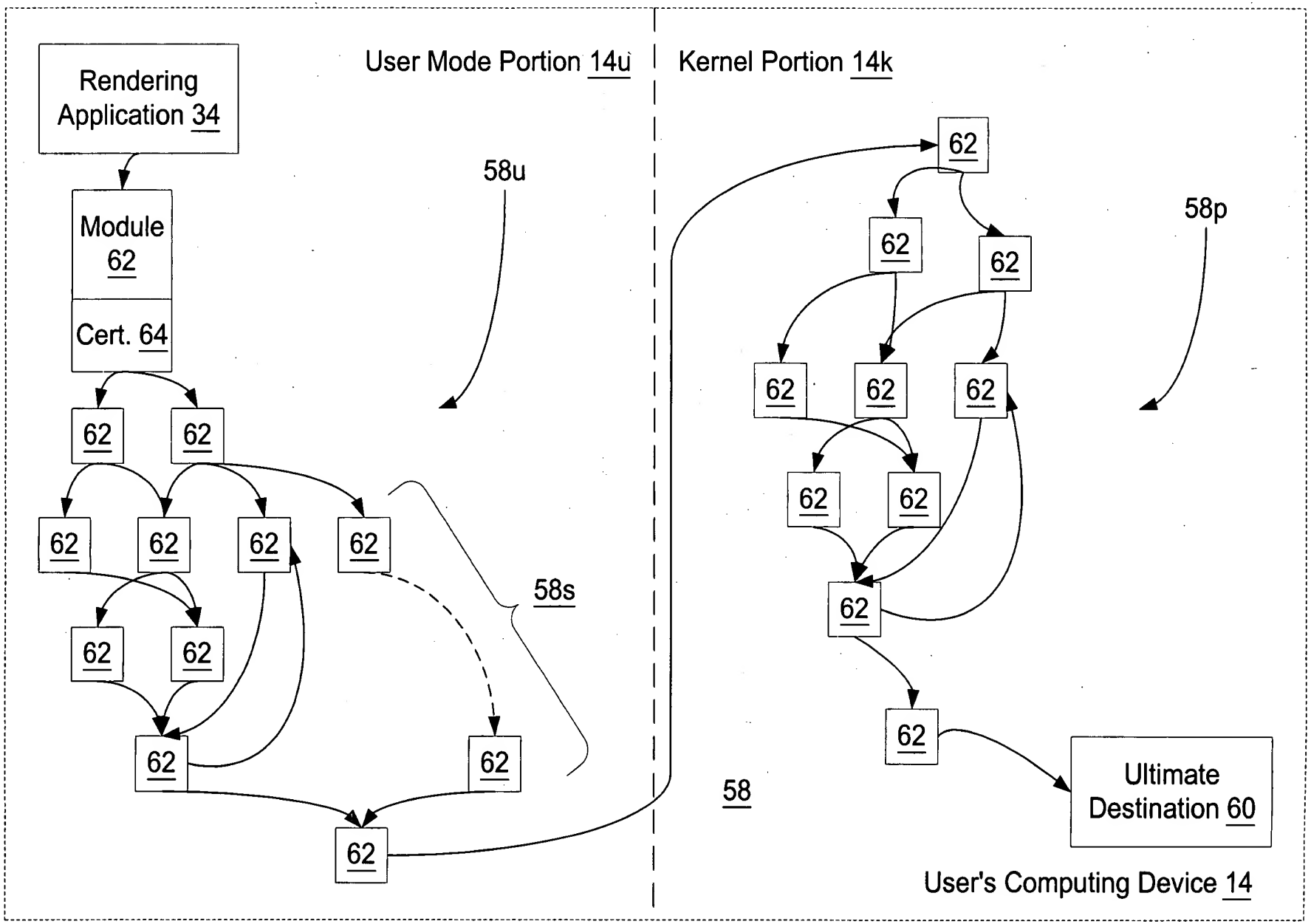
Rendering Application 34
User Mode Portion 14u
Kernel Portion 14k
Module 62
Cert. 64
58u
58p
58s
58
Ultimate Destination 60
User's Computing Device 14
62

Fig. 13

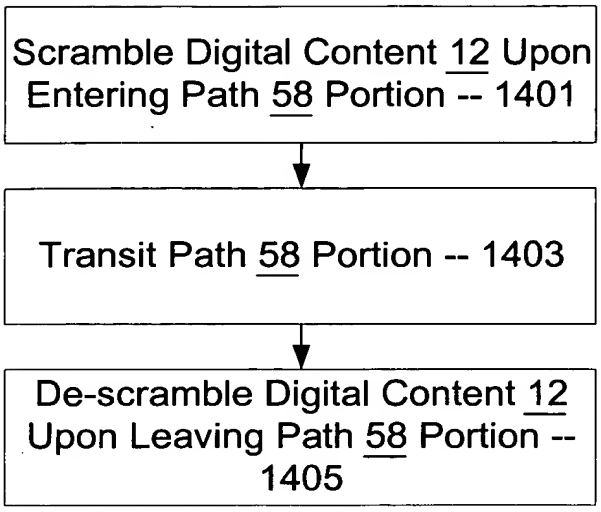

Fig. 14

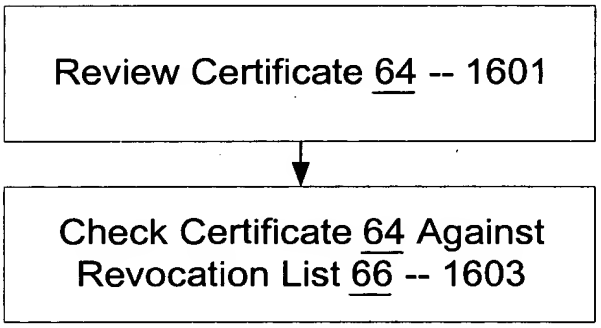

Fig. 16

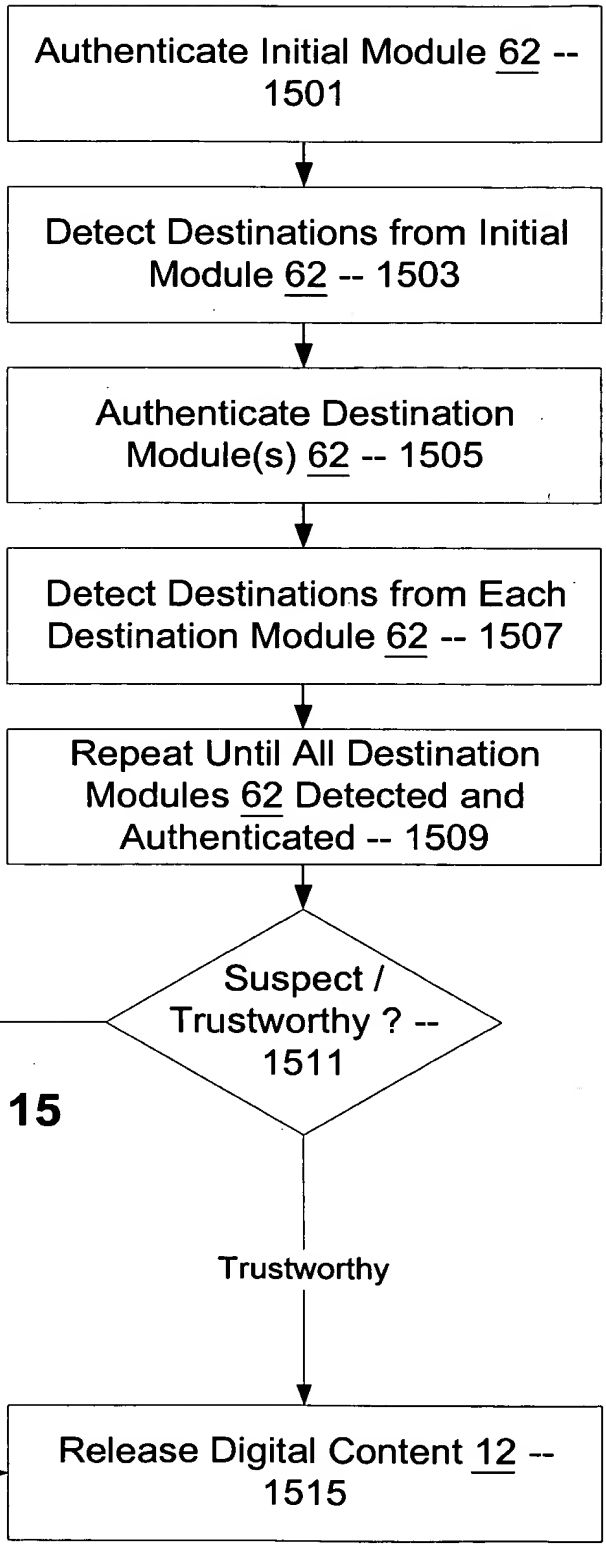

Fig. 15

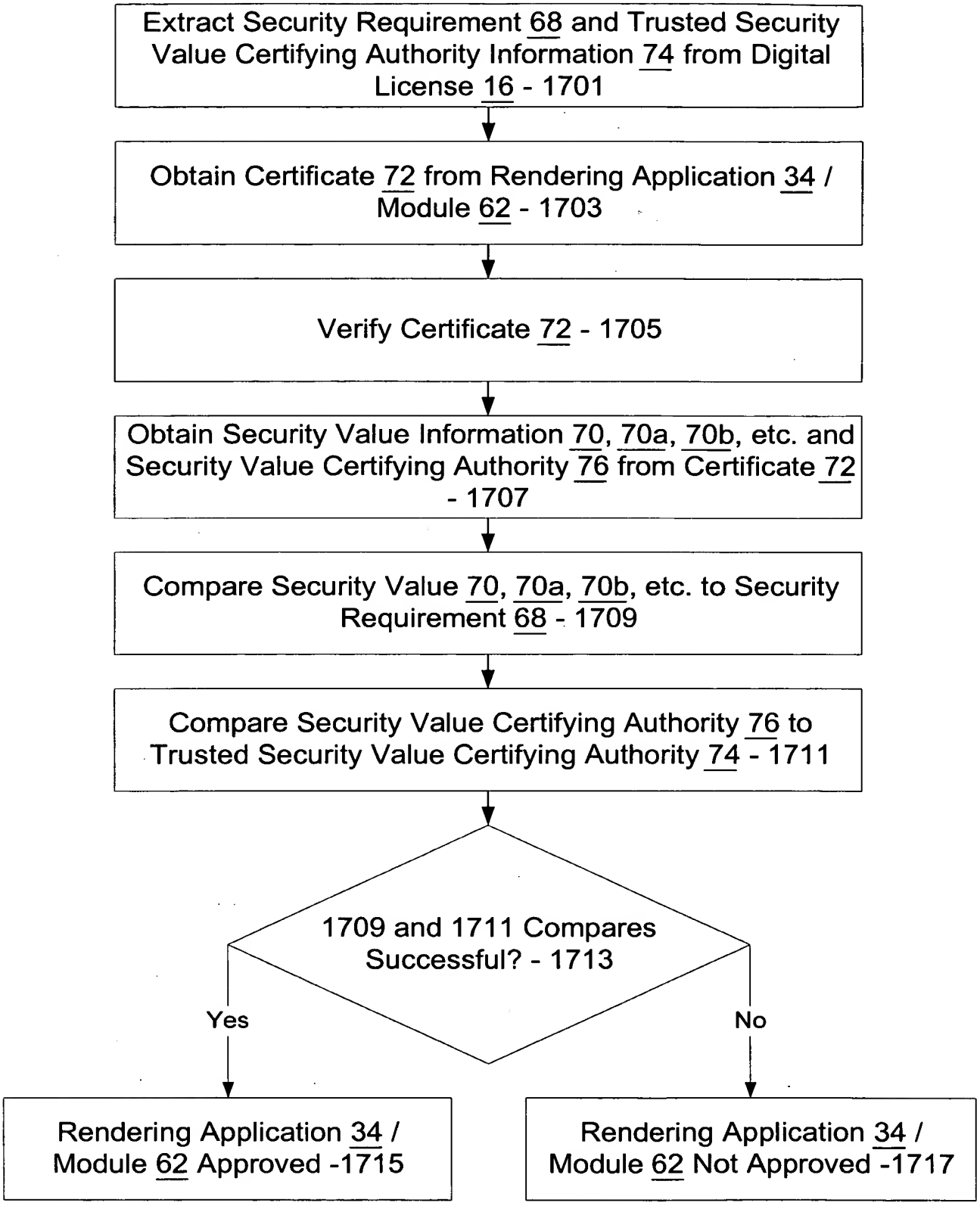
Extract Security Requirement 68 and Trusted Security Value Certifying Authority Information 74 from Digital License 16 - 1701
Obtain Certificate 72 from Rendering Application 34 / Module 62 - 1703
Verify Certificate 72 - 1705
Obtain Security Value Information 70, 70a, 70b, etc. and Security Value Certifying Authority 76 from Certificate 72 - 1707
Compare Security Value 70, 70a, 70b, etc. to Security Requirement 68 - 1709
Compare Security Value Certifying Authority 76 to Trusted Security Value Certifying Authority 74 - 1711
1709 and 1711 Compares Successful? - 1713
Yes
No
Rendering Application 34 / Module 62 Approved -1715
Rendering Application 34 / Module 62 Not Approved -1717

Fig. 17

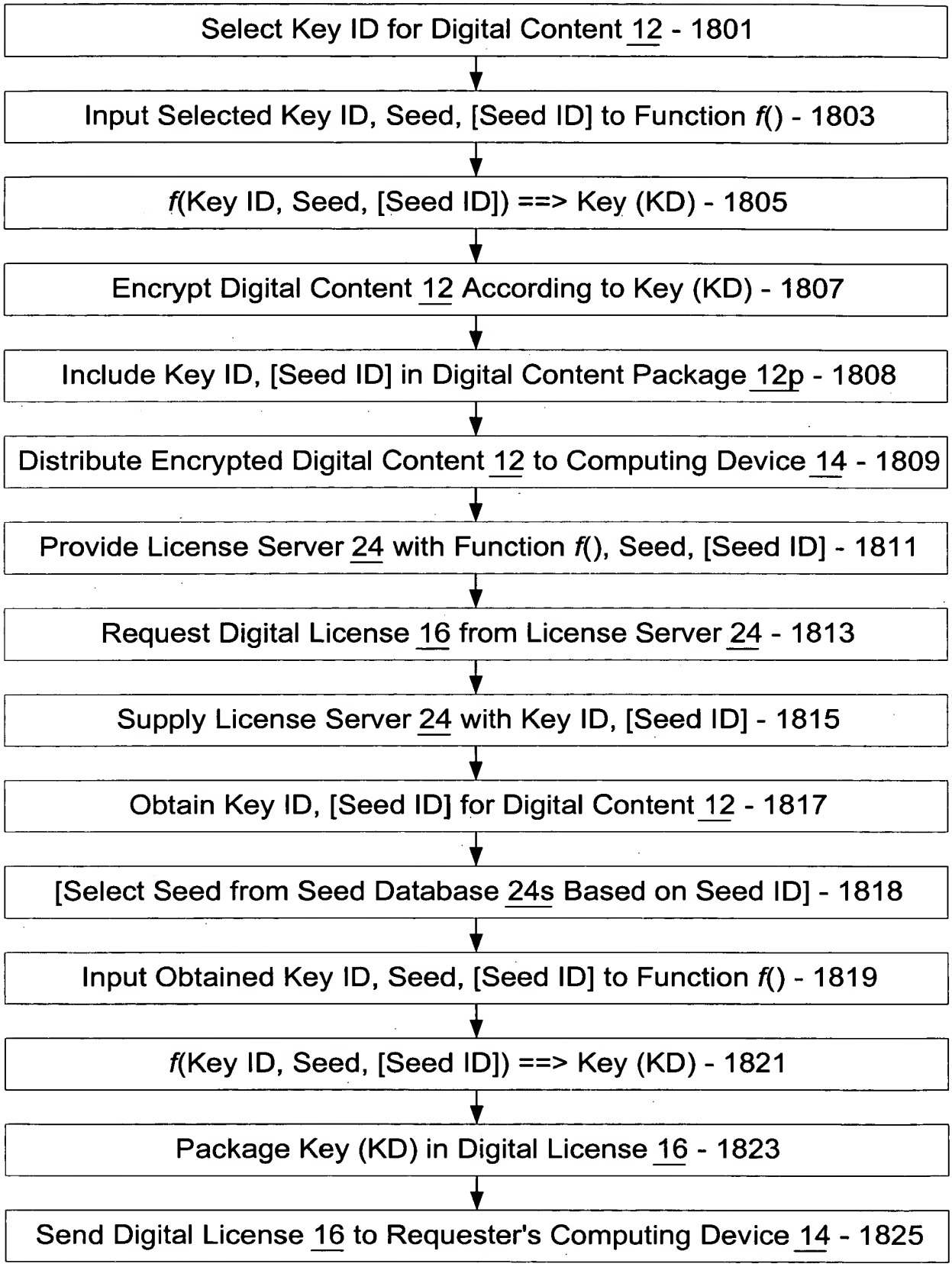
Select Key ID for Digital Content 12 - 1801
Input Selected Key ID, Seed, [Seed ID] to Function f() - 1803
f(Key ID, Seed, [Seed ID]) ==> Key (KD) - 1805
Encrypt Digital Content 12 According to Key (KD) - 1807
Include Key ID, [Seed ID] in Digital Content Package 12p - 1808
Distribute Encrypted Digital Content 12 to Computing Device 14 - 1809
Provide License Server 24 with Function f(), Seed, [Seed ID] - 1811
Request Digital License 16 from License Server 24 - 1813
Supply License Server 24 with Key ID, [Seed ID] - 1815
Obtain Key ID, [Seed ID] for Digital Content 12 - 1817
[Select Seed from Seed Database 24s Based on Seed ID] - 1818
Input Obtained Key ID, Seed, [Seed ID] to Function f() - 1819
f(Key ID, Seed, [Seed ID]) ==> Key (KD) - 1821
Package Key (KD) in Digital License 16 - 1823
Send Digital License 16 to Requester's Computing Device 14 - 1825

Fig. 18

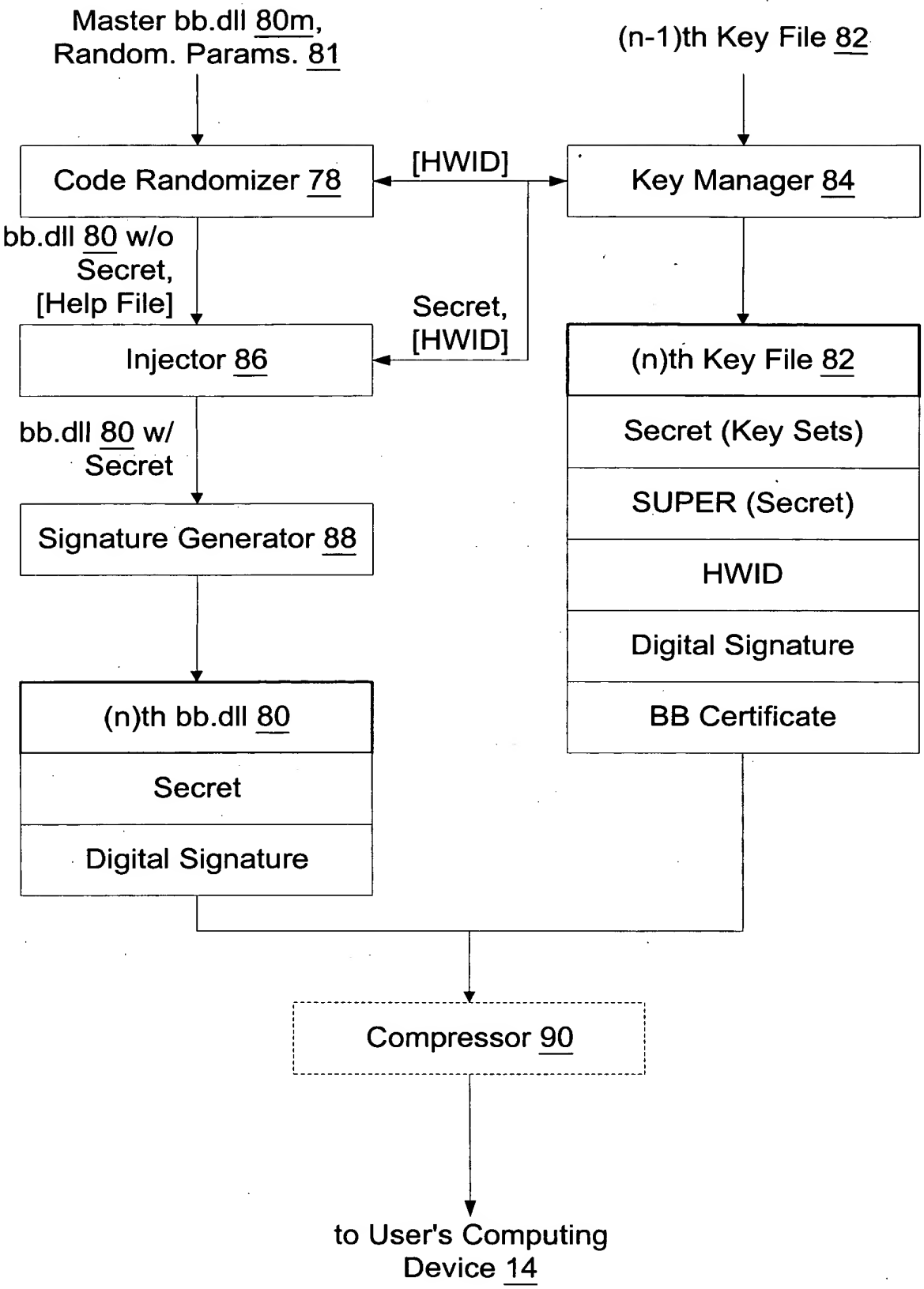
Master bb.dll 80m, Random. Params. 81
(n-1)th Key File 82
Code Randomizer 78
[HWID]
Key Manager 84
bb.dll 80 w/o Secret, [Help File]
Secret, [HWID]
Injector 86
(n)th Key File 82
Secret (Key Sets)
SUPER (Secret)
HWID
Digital Signature
BB Certificate
bb.dll 80 w/ Secret
Signature Generator 88
(n)th bb.dll 80
Secret
Digital Signature
Compressor 90
to User's Computing Device 14

Fig. 19

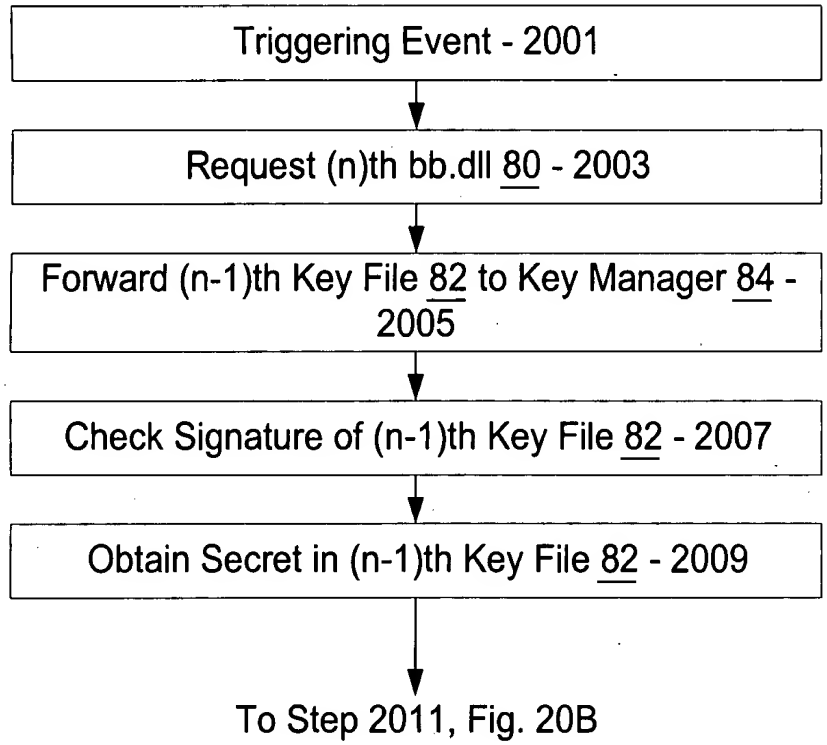

Fig. 20A

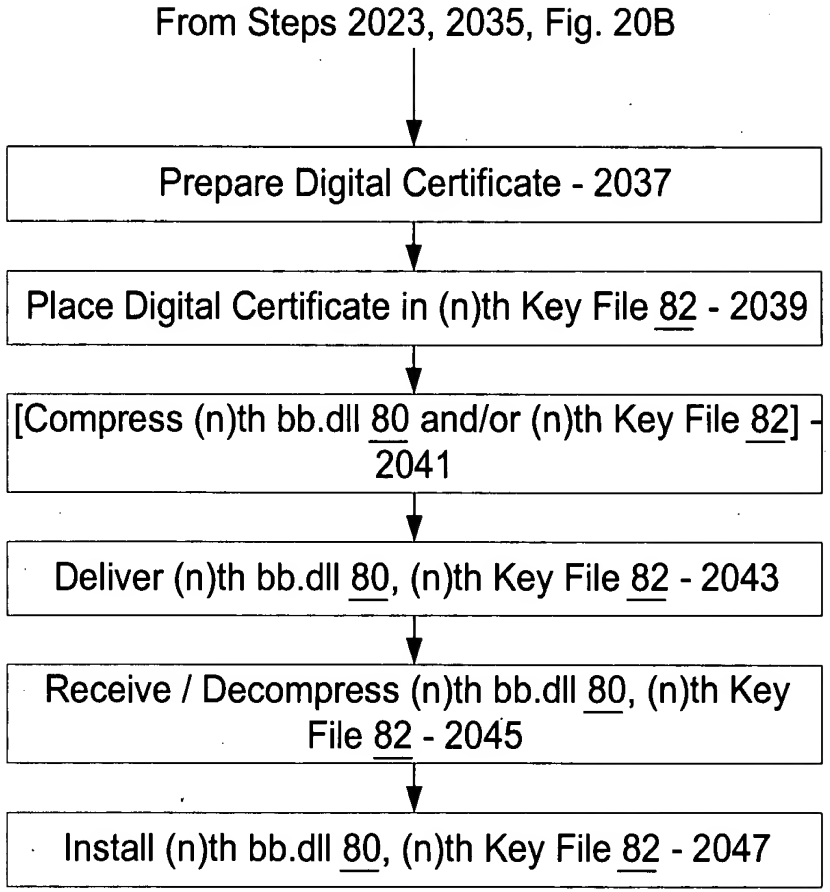

Fig. 20C

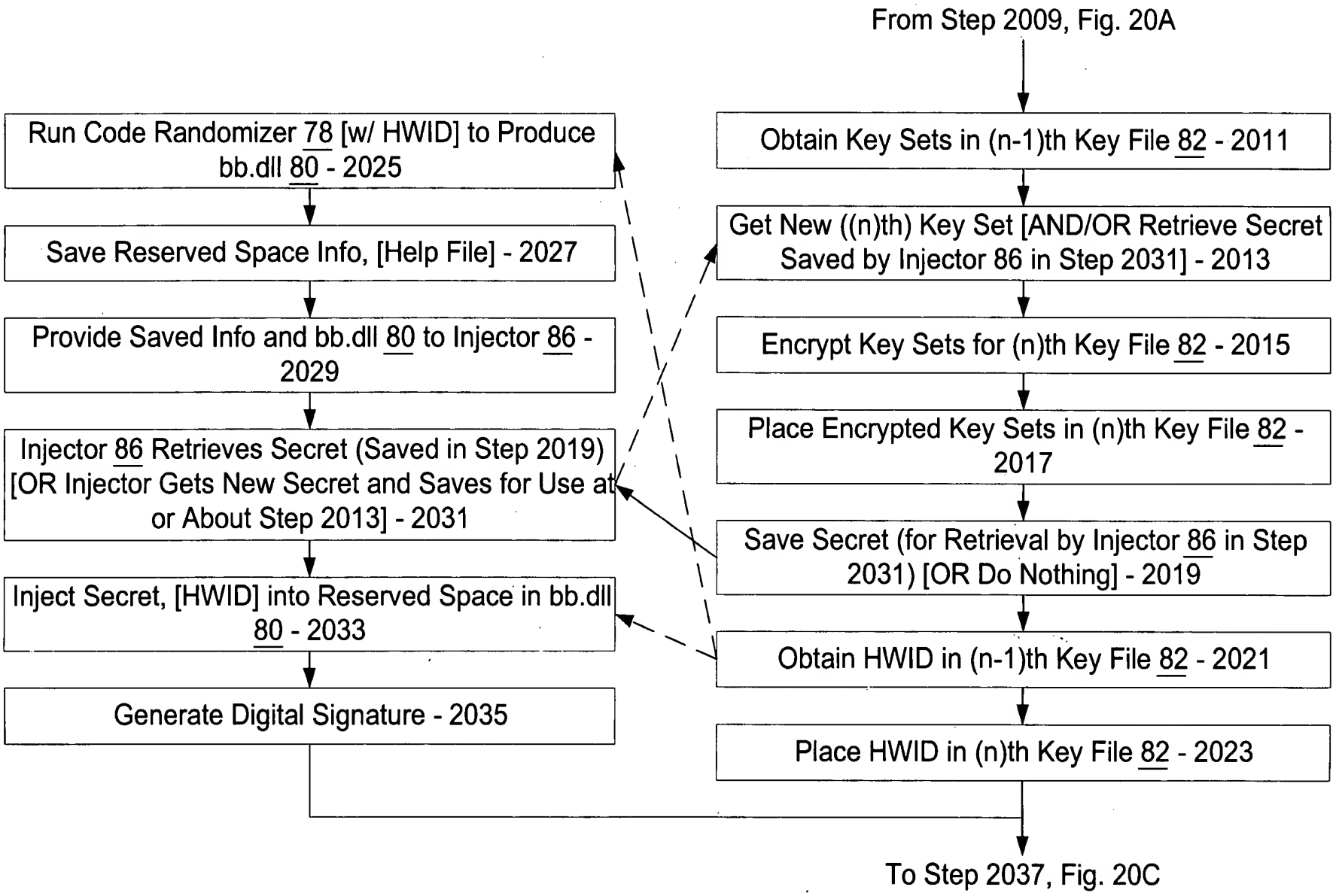
From Step 2009, Fig. 20A
Obtain Key Sets in (n-1)th Key File 82 - 2011
Get New ((n)th) Key Set [AND/OR Retrieve Secret Saved by Injector 86 in Step 2031] - 2013
Encrypt Key Sets for (n)th Key File 82 - 2015
Place Encrypted Key Sets in (n)th Key File 82 - 2017
Save Secret (for Retrieval by Injector 86 in Step 2031) [OR Do Nothing] - 2019
Obtain HWID in (n-1)th Key File 82 - 2021
Place HWID in (n)th Key File 82 - 2023
Run Code Randomizer 78 [w/ HWID] to Produce bb.dll 80 - 2025
Save Reserved Space Info, [Help File] - 2027
Provide Saved Info and bb.dll 80 to Injector 86 - 2029
Injector 86 Retrieves Secret (Saved in Step 2019) [OR Injector Gets New Secret and Saves for Use at or About Step 2013] - 2031
Inject Secret, [HWID] into Reserved Space in bb.dll 80 - 2033
Generate Digital Signature - 2035
To Step 2037, Fig. 20C

Fig. 20B

POSTED: 07/23/2008

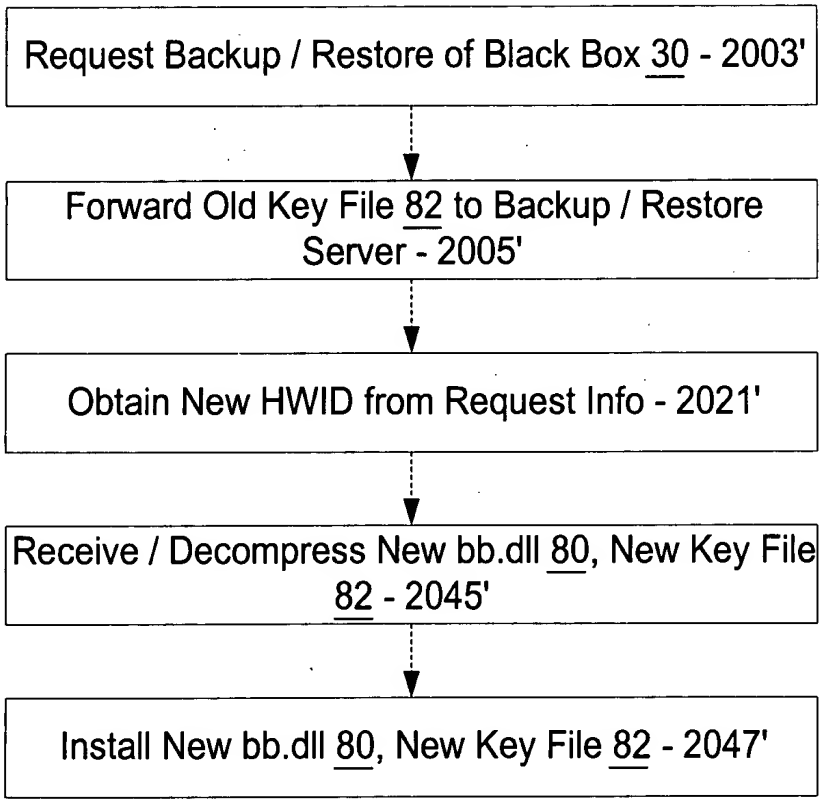

Fig. 20D

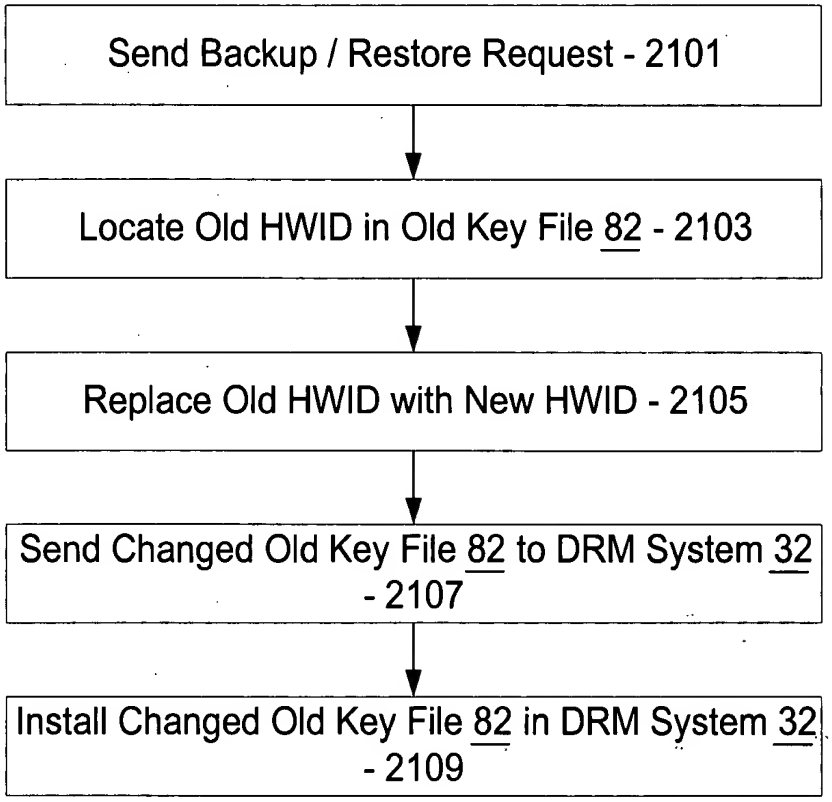

Fig. 21

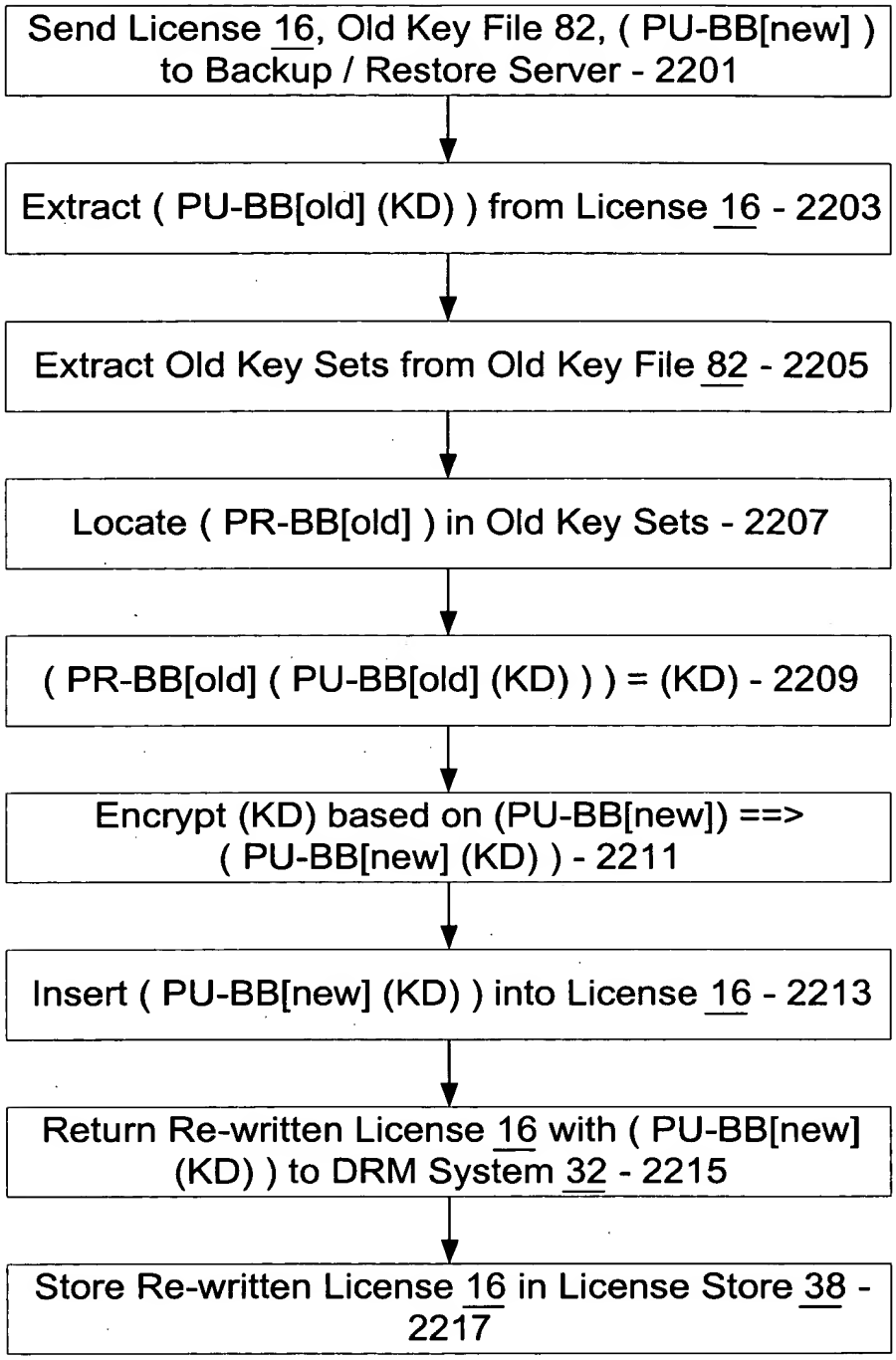
Send License 16, Old Key File 82, (PU-BB[new]) to Backup / Restore Server - 2201
Extract (PU-BB[old] (KD)) from License 16 - 2203
Extract Old Key Sets from Old Key File 82 - 2205
Locate (PR-BB[old]) in Old Key Sets - 2207
(PR-BB[old] (PU-BB[old] (KD))) = (KD) - 2209
Encrypt (KD) based on (PU-BB[new]) ==> (PU-BB[new] (KD)) - 2211
Insert (PU-BB[new] (KD)) into License 16 - 2213
Return Re-written License 16 with (PU-BB[new] (KD)) to DRM System 32 - 2215
Store Re-written License 16 in License Store 38 - 2217

Fig. 22